AMENDMENTS TO THE CLAIMS:

Please amend claims 1, 11, 17 and 20 as follows.

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (currently amended) A network bridge, said network bridge including ~~having~~ a malware scanner.

2. (original) A network bridge as claimed in claim 1, comprising a data packet analyser operable to identify data packets received by said network bridge at least a portion of which are to be passed to said malware scanner for scanning.

3. (original) A network bridge as claimed in claim 2, wherein said data packet analyser identifies data packets having a predetermined network layer protocol as to be passed to said malware scanner for scanning.

4. (original) A network bridge as claimed in claim 3, wherein said predetermined network layer protocol is one or more of:

TCP/IP;

IPX;

SNA; and

Appletalk.

5. (original) A network bridge as claimed in claim 2, wherein said data packet analyser identifies data packets having a predetermined application layer protocol as to be passed to said malware scanner for scanning.

6. (original) A network bridge as claimed in claim 5, wherein said predetermined application layer protocol is one or more of:

SMTP;

FTP;

HTTP;

SMB; and

NFS.

7. (original) A network bridge as claimed in claim 1, wherein said malware scanner is operable to concatenate portions of a data file from a plurality of data packets to form a data file to be scanned.

8. (original) A network bridge as claimed in claim 1, wherein said malware scanner is operable to scan for one or more of:

computer viruses;

Trojans;

worms;

banned computer programs; and

banned words within e-mail messages.

9. (original) A network bridge as claimed in claim 1, wherein data that has been scanned by said malware scanner is forwarded to its intended recipient.

10. (original) A network bridge as claimed in claim 1, wherein said malware scanner is formed of one or more of:

a software based malware scanner; and

a hardware based malware scanner.

11. (currently amended) A network bridge comprising:

~~operable to intercept~~means for intercepting at least one ~~or more~~ data packet~~s~~,

~~to forward~~means for forwarding at least a portion of said at least one data packet~~s~~ to a malware scanner for scanning, and

~~to forward~~means for forwarding data from said at least one data packet~~s~~ after scanning to ~~its~~an intended recipient.

12. (original) A network bridge as claimed in claim 11, comprising a data packet analyser operable to identify data packets received by said network bridge at least a portion of which are to be passed to said malware scanner for scanning.

13. (original) A network bridge as claimed in claim 12, wherein said data packet analyser identifies data packets having a predetermined network layer protocol as to be passed to said malware scanner for scanning.

14. (original) A network bridge as claimed in claim 13, wherein said predetermined network layer protocol is one or more of:

TCP/IP;

IPX;

SNA; and

Appletalk.

15. (original) A network bridge as claimed in claim 12, wherein said data packet analyser identifies data packets having a predetermined application layer protocol as to be passed to said malware scanner for scanning.

16. (original) A network bridge as claimed in claim 15, wherein said predetermined application layer protocol is one or more of:

SMTP;

FTP;

HTTP;

SMB; and

NFS.

17. (currently amended) A malware scanner in combination with a network bridge, comprising:

~~operable to receive~~means for receiving at least a portion of at least one ~~or more~~ data packet~~s~~ intercepted by ~~a~~said network bridge,

~~to concatenate~~means for concatenating said at least one data packet~~s~~ into a data file to be scanned, and

~~to forward~~means for forwarding said data file after scanning to ~~its~~an intended recipient~~s~~ via said network bridge.

18. (original) A malware scanner as claimed in claim 17, wherein said malware scanner is operable to scan for one or more of:

computer viruses;

Trojans;

worms;

banned computer programs; and

banned words within e-mail messages.

19. (original) A malware scanner as claimed in claim 17, wherein said malware scanner is formed of one or more of:

a software based malware scanner; and

a hardware based malware scanner.

20. (currently amended) A method of malware scanning comprising the steps of:

receiving at least one data packet~~s~~ at a network bridge;

sending at least a portion of said at least one data packets from said network bridge to a malware scanner;

concatenating data received by said malware scanner to form a data file to be scanned;

scanning said data file with said malware scanner; and

forwarding said data file after scanning via said network bridge to ~~its~~an intended recipient.

21. (original) A method as claimed in claim 20, comprising the step of identifying data packets received by said network bridge that are to be passed to said malware scanner for scanning.

22. (original) A method as claimed in claim 21, wherein data packets having a predetermined network layer protocol are identified as to be passed to said malware scanner for scanning.

23. (original) A method as claimed in claim 22, wherein said predetermined network layer protocol is one or more of:

TCP/IP;

IPX;

SNA; and

Appletalk.

24. (original) A method as claimed in claim 21, wherein data packets having a predetermined application layer protocol are identified as to be passed to said malware scanner for scanning.

25. (original) A method as claimed in claim 24, wherein said predetermined application layer protocol is one or more of:

SMTP;

FTP;

HTTP;

SMB; and

NFS.

26. (original) A method as claimed in claim 20, wherein said scanning scans for one or more of:

computer viruses;

Trojans;

worms;

banned computer programs; and

banned words within e-mail messages.

27. (original) A method as claimed in claim 20, wherein said malware scanner is formed of one or more of:

a software based malware scanner; and

a hardware based malware scanner.